UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,607	06/01/2001	Christophe Clavier	032326-132	2078

21839 7590 08/28/2006

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 08/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/807,607	CLAVIER ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 13-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 13-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on June 21, 2006. Claims 1-10, and 13-16 are still pending consideration.

Response to Arguments

2. Applicant's arguments filed June 21, 2006 have been fully considered but they are not persuasive for the following reasons:

The Applicant argues that the Cited Prior Art (CPA), Kocher et al. (U.S. Patent No. 6,278,783) in view of Chow et al. (U.S. Patent No. 6,594,761), does not teach a first manipulating means and a other manipulating means that are derived from said first manipulating means. This argument is not found persuasive. Kocher teaches a method of permutating a message with an initial key and initial permutations before the round functions use subkeys, which are generated from the initial key, to update the message and provide a final message permutations (Figure 1). Therefore, the initial permutations is interpreted as the first manipulating means, and the other manipulating means derived from the first manipulating means are the subkeys which are derived from the initial key, and used to form the final message permutation.

Regarding claim 13, the Applicant argues that the CPA does not teach "a means for generating a random value for selecting the manipulating means to be employed

during a given execution of said algorithm." This argument is not found persuasive. Chow discloses that the encoding using one of the delineated techniques including complementation can be random "so the encoding chosen for the data is not exposed" (column 19 lines 60-64). Therefore, it is respectfully asserted that the CPA does teach "a means for generating a random value for selecting the manipulating means to be employed during a given execution of said algorithm." Therefore, the rejection for the pending claims is respectfully maintained as given below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-10 and 13-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. (U.S Patent no. 6, 278, 783) in view of Chow et al. (U.S. Patent No. 6,594,761).

Regarding claim 1, Kocher discloses:

A countermeasure method against attacks by differential analysis of current consumption in an electronic component using a cryptographic algorithm having a secret key, comprising the following steps:

"***executing a first set of instructions in the algorithm that are critical to said attacks with a first manipulating means to deliver output data on the basis of input data***" (Figures 1 and 2; column 1, line 66 – column 2, line 24);

"***executing another set of said critical instructions with other manipulating means that are derived from said first manipulating means"*** (Figures 1 and 2; column 1, line 66 – column 2, line 24). Kocher does not explicitly disclose that this manipulating means is by "***complementation of at least one of the input data and said output data, so that the output data and the data derived from said output data are unpredictable***." Chow discloses a tamper-proofing encoding method that can be used with encryption protocols (see description of application of the method to DES, starting at column 20, line 28). Chow further discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50 – column 19, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the method disclosed by Kocher by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (Chow, column 4, lines 3-9).

Claim 2 is rejected as applied above in rejecting claim 1. Kocher does not explicitly teach that "***first and other manipulating means are selected for use on the basis of one-half probability statistical relationship.***" Chow discloses randomly selecting whether to perform an operation or its complement (column 18, line 50 – column 19, line

13), which provides a one-half probability statistical relationship. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the method disclosed by Kocher by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (Chow, column 4, lines 3-9).

Claim 3 is rejected as applied above in rejecting claim 2. Kocher does not explicitly disclose a countermeasure method, wherein said "***method comprises executing a first sequence and a second sequence, such that the order in which the sequences are executed is a function of the one-half probability statistical relationship.***" Chow discloses randomly selecting whether to perform an operation or its complement (column 18, line 50 – column 19, line 13), which provides a one-half probability statistical relationship. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the method disclosed by Kocher by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (Chow, column 4, lines 3-9).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Kocher discloses:

A countermeasure method according to claim 3, wherein "***each of the first and second sequences is made up of the first three rounds***" (column 4 lines 47-65),

wherein the encryption operators can be of any type including DES, and further, can include any number of rounds that are in each of the respective encryption operators.

Claim 5 is rejected as applied above in rejecting claim 3. Furthermore, Leppek discloses:

A countermeasure method according to claim 3. Kocher does not explicitly state ***"other manipulating means consist of second means such that, for the same input data, the complement of the output data of the first manipulating means is produced as output data."*** Chow discloses a tamper-proofing encoding method that can be used with encryption protocols (see description of application of the method to DES, starting at column 20, line 28). Chow further discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50 – column 19, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the method disclosed by Kocher by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (Chow, column 4, lines 3-9).

Claim 6 is rejected as applied above in rejecting claim 2. Furthermore, Kocher discloses the use of a modified DES encryption algorithm which consists of sixteen rounds (Figure 1). Kocher does not explicitly disclose a countermeasure method, wherein said "***method comprises executing a first sequence and a second sequence, such that the order in which the sequences are executed is a function***

of the one-half probability statistical relationship." Chow discloses randomly selecting whether to perform an operation or its complement (column 18, line 50 – column 19, line 13), which provides a one-half probability statistical relationship. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the method disclosed by Kocher by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (Chow, column 4, lines 3-9).

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Kocher discloses:

A countermeasure method according to claim 6, wherein "***each of the first and second sequences is made up of the last three rounds***" (column 4 lines 47-65), wherein the encryption operators can be of any type including DES, and further, can include any number of rounds that are in each of the respective encryption operators; Kocher does not explicitly disclose "***wherein the other manipulating means used in the second sequence comprise second manipulating means and a third manipulating means***" Chow discloses a tamper-proofing encoding method that can be used with encryption protocols (see description of application of the method to DES, starting at column 20, line 28). Chow further discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50 – column 19, line 13), or a multiple of other operations (third manipulating means) which "results in a substantial increase in the number of operations relative to

the original program" (Chow: column 19 lines 13-17). Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the method disclosed by Kocher by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (Chow, column 4, lines 3-9).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Kocher discloses:

A countermeasure method according to claim 7, wherein "***said second manipulating means are used in the second sequence for the fourteenth round***" (column 4 lines 47-65), wherein the encryption operators can be of any type including DES, and further, can include any manipulation in any of the rounds, including the fourteenth round of the respective encryption operation. Kocher does not explicitly disclose ***"second manipulating means are such that, for the same input data, the complement of the output data of the first manipulating means is produced as output data.***" Chow discloses a tamper-proofing encoding method that can be used with encryption protocols (see description of application of the method to DES, starting at column 20, line 28). Chow further discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50 – column 19, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the method disclosed by Kocher by

performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (Chow, column 4, lines 3-9).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Kocher discloses:

A countermeasure method according to claim 8, wherein "said third manipulating means are used in the second sequence for the fifteenth and the sixteenth round" (column 4 lines 47-65), wherein the encryption operators can be of any type including DES, and further, can include any manipulation in any of the rounds, including the fourteenth round of the respective encryption operation. Kocher does not explicitly disclose ***"second manipulating means are such that, for the same input data, the complement of the output data of the first manipulating means is produced as output data."*** Chow discloses a tamper-proofing encoding method that can be used with encryption protocols (see description of application of the method to DES, starting at column 20, line 28). Chow further discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50 – column 19, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the method disclosed by Kocher by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (Chow, column 4, lines 3-9).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Kocher discloses:

A countermeasure method according to claim 1, wherein "***manipulating means are constants tables***" (column 7, lines 15-65). Kocher teaches the use of tables to manipulate data (column 7 lines 15-65), wherein the tables are used as a method to minimize information leakage when using a electric component such as a smart card. The tables are filled with parameters (constants), which are preferably updated so that attackers cannot obtain the contents of the table by analysis of measurements.

Regarding claim 13, Kocher discloses:

An electronic component which provides countermeasures against attacks on a secret key cryptographic algorithm, comprising:

"***a program memory having stored therein a plurality of different manipulating means for producing output data in response to input data***" (Figures 1 and 2; column 1, line 66 – column 2, line 24);

"***a processor which executes instructions in said algorithm that are critical to said attacks, in accordance with a selected one of said manipulating means***" (Figures 1 and 2; column 1, line 66 – column 2, line 24); and

Kocher does not explicitly teach "***means for generating a random value for selecting the manipulating means to be employed during a given execution of said algorithm, such that output data produced thereby is unpredictable.***" Chow discloses a tamper-proofing encoding method that can be used with encryption

protocols (see description of application of the method to DES, starting at column 20, line 28). Chow further discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50 – column 19, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the method disclosed by Kocher by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (Chow, column 4, lines 3-9).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Leppek discloses:

A countermeasure method according to claim 13, wherein "***manipulating means are constants tables***" (column 7, lines 15-65). Kocher teaches the use of tables to manipulate data (column 7 lines 15-65), wherein the tables are used as a method to minimize information leakage when using a electric component such as a smart card. The tables are filled with parameters (constants), which are preferably updated so that attackers cannot obtain the contents of the table by analysis of measurements.

Claim 15 is rejected as applied above in rejecting claim 13. Kocher does not explicitly disclose that "***different manipulating means respectively produce sets of output data that are complementary to one another***." Chow discloses a tamper-proofing encoding method that can be used with encryption protocols (see description of application of the method to DES, starting at column 20, line 28). Chow further

discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50 – column 19, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the method disclosed by Kocher by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (Chow, column 4, lines 3-9).

Claim 16 is rejected as applied in rejecting claim 13. Furthermore, Kocher discloses:

The electronic component of claim 13, "***wherein said component is a smart card***" (see Abstract).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 703-305-8892. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

KA
08/24/2006